IAMとアイデンティティ・セキュリティ製品を同じベンダーから購入するとどうなるか

March 10, 2022 | Venu Shastri | アイデンティティ保護

＊原文は CrowdStrike Blog サイト掲載：
https://www.crowdstrike.com/blog/why-you-shouldnt-buy-iam-and-identity-security-from-the-same-vendor/

最近のランサムウェアやサプライチェーン攻撃に見られるようなアイデンティティを基点とした侵害のリスクが高まるなか、企業はアイデンティティ・セキュリティの必要性を認識し始めています。企業がアイデンティティ保護の強化に対する最善の方法を検討する際に、アイデンティティ管理やアイデンティティ/アクセス管理（IAM）製品を提供するベンダーの企業向けバンドルに含まれるセキュリティ機能やモジュールで済ませようとする傾向が見られます。

たとえば、Microsoft E3/E5を導入し、アイデンティティレイヤーとしてActive DirectoryやAzure ADを既に使用しているケースは一般的ですが、このような組織がアイデンティティ・セキュリティのニーズに対応するために、Microsoft Defender for IdentityやAzure AD Identity Protectionを選択することがあります。

同じベンダーの複数の製品を、企業向けバンドルの一部として使用すれば、通常は高い費用対効果が見込めますが、多額の損失をもたらすような壊滅的な侵害が発生するケースもあります。アイデンティティソリューションとアイデンティティ・セキュリティソリューションの組み合わせはその一例です。多くの利用者はアイデンティティ・セキュリティソリューションがどのような機能を持つべきかを十分に理解していません。

そのような同一ベンダー製品の組み合わせがなぜ問題なのかを説明する前に、いくつかの定義について確認してみましょう。

IAMとアイデンティティ・セキュリティの違い

IAMは、組織のITセキュリティ戦略の一部であり、デジタルアイデンティティおよびデータ、システム、その他のリソースへのユーザーアクセスの管理に重点を置くものです。IAM技術では、アイデンティティの保管や管理、シングルサインオン（SSO）や多要素認証（MFA）機能を提供します。このように、本来侵害を検知・防御するためのセキュリティソリューションとして設計されているものではありません。

一方、アイデンティティ・セキュリティは、アイデンティティに起因する侵害（特に攻撃者が従来型のセキュリティ対策を回避しようとする動きをする際）を検知し防御することのみを目的として構築された包括的なソリューションです。理想的なアイデンティティ・セキュリティソリューションは、エンドポイント、クラウドワークロード、アイデンティティ、データなど、侵害にさらされる企業ネットワークのあらゆる層を詳細に可視化し、より正確な検知と対応を可能にする「包括的なセキュリティプラットフォームの一部」であるべきです。

同じベンダーからIAMとアイデンティティ・セキュリティ製品を購入することの落とし穴

利益相反

サイバーセキュリティ製品の購入を決定する際に、ベンダーの利害関係があるような分野の組み合わせは避けるべきです。しかし、これは意外と見過ごされています。責任範囲は明確に分離されるべきです。たとえば、会計においては、監査人が独立した検

査を行って数字が正しいことを確認します。またソフトウェア開発では、開発者が書いたコードのテストが行われます。同じ概念はセキュリティにも当てはまります。アイデンティティ管理製品とアイデンティティ・セキュリティ製品を同じベンダーから購入した場合、「中立性の確保」という基本的な考え方を無視することになります。

Microsoft Active Directoryは、数十年前のレガシーテクノロジーを基盤に構築されており、組織のサイバー防衛戦略における最大の抜け穴となるひとつであると考えられています。**Active Directoryの新しい脆弱性は毎年発見されており**、最近では**数秒のうちにドメイン全体を侵害できる脆弱性**も検出されています。また、Active Directoryは最も広く利用されているアイデンティティストアの一つであり、**Fortune 1000企業の90%以上が現在も利用している**ことから、アイデンティティベースの攻撃の対象として非常に狙われやすくなっています。

マイクロソフトは、アイデンティティ管理ベンダーとして、Active Directoryの脆弱性に対するパッチを顧客に提供する義務がありますが、それは単に必須の役目でしかありません。同社がアイデンティティ・セキュリティベンダーでもあるならば、その製品の脆弱性を突く攻撃を仕掛けられないように、検知と修復の機能も速やかに提供すべきです。しかし、マイクロソフトはこの領域において**何度も顧客を失望させてきました**。

これに対し、CrowdStrikeのように、中立的でセキュリティに特化したベンダーがアイデンティティ・セキュリティを提供する場合、このような利害の相反はなくなります。CrowdStrikeの目的とするところは、アイデンティティ製品の脆弱性にパッチを当てることではありません、唯一の目的は、侵害から顧客を保護し、プロアクティブな検知と修復の能力を提供することです。

連携においても利益相反の問題は生じます。アイデンティティ・セキュリティ製品は、広範なアイデンティティ製品との連携機能と可視化機能を備え、アイデンティティの総合的な可視性を提供できる必要があります。しかし、アイデンティティベンダーがアイデンティティ・セキュリティレイヤーも提供している場合、わざわざ他のアイデンティティベンダーと連携してまで、ハイブリッド環境内の複数のアイデンティティストアを可視化できる統合インターフェイスを提供しようとは考えないでしょう。一方、CrowdStrike Falcon®製品は、Active DirectoryやAzure ADだけでなく、Okta、Ping、Duo、CyberArkなどの他の優れたIAM/MFAベンダーとも連携しており、マイクロソフト主体のMicrosoft Defender for Identityとの違いは歴然です。

セキュリティ層の薄さ

「アイデンティティ・セキュリティ」には「アイデンティティ」という言葉が含まれていますが、重視すべきはセキュリティです。理想的なアイデンティティ・セキュリティソリューションは、広範なセキュリティプラットフォームの一部であり、複数のソースからのセキュリティ情報を関連付けできるものであるべきです。

CrowdStrike Security Cloudは、1日あたり何兆件ものセキュリティイベントを、Indicators of Attack（IOA：攻撃の兆候）、業界をリードする脅威インテリジェンス、および顧客のエンドポイント、ワークロード、アイデンティティ、データから得たテレメトリ情報と関連づけることができます。Falconソリューションは、セキュリティにこだわり、さまざまな攻撃データを取り込むことで、超高精度の検知機能と自動化された保護・修復機能を実現しています。

マイクロソフトのような巨大ソフトウェア企業は、レガシー製品による長年の甚大な技術的負債を抱えながら、クラウドインフラやクラウドサービス、ソフトウェア、ハードウェア、ゲームに至るまで、さまざまな新しい製品を提供しているため、セキュリティに対し集中的に取り組むことは困難です。クラウド以前の時代からのレガシーアプローチを取るマイクロソフトは、その製品上で新たに発見される脆弱性を修正しようと常に必死になっています。同社は長年にわたり、**Active Directoryサプライチェーンの侵害**や**PrintNightmare**の脆弱性、攻撃者による**Active Directoryで一般的に生じる不適切な設定**の悪用など、セキュリティ上の問題を相次いで経験してきました。

この種の弱点は、最近の**noPacエクスプロイト**でも狙われました。これは、Active Directoryに関係する重要なCVE（CVE-2021-42278とCVE-2021-42287）を組み合わせて悪用し、侵害したドメインへのダイレクトパスを利用して権限昇格を行うものです。**CrowdStrike Falcon Identity Threat Protection**では、このような脆弱性の悪用を自動的に検知し、シンプルなポリシーを適用してMFAを強制することでnoPacをブロックできます。一方マイクロソフトは、自社の製品内の脆弱性に対応するパッチを提供したものの、それらを各ADドメインコントローラーに適用する作業自体は顧客への負担となっています。

ベンダーロックイン

アイデンティティレイヤーを提供するベンダーが、クラウドインフラストラクチャーも提供しており、顧客を自社クラウドに移行させる既得権を保有している場合、利害関係はさらに複雑になります。

オンプレミスのアイデンティティレイヤー（Active Directoryなど）に新たな脆弱性やアーキテクチャ上の欠陥が発見された場合、脆弱性を回避するためにクラウドアイデンティティレイヤー（Azure ADなど）に移行することをベンダーが顧客に提案してくるかもしれません。しかし、既にADインフラストラクチャ上にアプリケーションを構築しており、移行に数年を要する顧客にとって、それは事実上不可能です。そして何より、クラウドに移行しただけでは、ADの脆弱性を悪用して大損害を与えようとする攻撃者から守ることはできないのです。

興味深いことに、**マイクロソフトの最近のレポート**では、Azure ADにおけるMFAの採用率は依然として低く、Azure ADのアイデンティティとして要求されるのは、ほぼユーザー名とパスワードのみであることが明らかにされ、Azure ADがADのセキュリティ上の問題を解決する特効薬ではないことを浮き彫りにしています。

ベンダーロックインは、今日のマルチクラウド環境を活用することを妨げ、顧客に損害を与える場合もあります。特定のクラウドインフラに顧客を誘導するような利害関係を持たないCrowdStrikeのように中立的なベンダーのアイデンティティ・セキュリティソリューションを利用することで、そのような問題に対処することができます。また、ハイブリッドクラウドに移行する企業も、移行期間中の侵害を心配することなく、じっくりと計画・実施する時間を取ることができるでしょう。

最後に、複数のアイデンティティベンダーを使うセキュリティアプローチでは、企業がMFAプロバイダーを柔軟に選択することができます。CrowdStrike Falconアイデンティティ保護ソリューションは、Okta、Duo、Google Authenticatorなどの主要なMFAプロバイダーと簡単に連携できるため、マイクロソフト製品のように1つのMFAソリューションに縛られることなく、煩わしさのないMFA体験を実現します。

アイデンティティ・セキュリティとID管理を分離すべき理由

ランサムウェアのような昨今の攻撃は、アイデンティティを基点とする場合が多いため、強力なアイデンティティ・セキュリティソリューションをセキュリティ体制の重要な構成要素として組み込む必要があります。アイデンティティベンダーのエンタープライズバンドルに含まれるアイデンティティ・セキュリティソリューションで妥協するならば、セキュリティ性能が低下し、侵害のリスクが高まる可能性があります。アイデンティティ・セキュリティのニーズには、エンドポイント、クラウドワークロード、アイデンティティ、データなど、企業のリスクに関係するすべての重要な領域を保護できる、中立的なセキュリティベンダー提供のソリューションがより役立つでしょう。

その他のリソース

- CrowdStrike Falconアイデンティティ保護ソリューション で従業員のアイデンティティを保護することにより、組織全体のコストとリスクをどのように低減できるかをご覧ください。
- Falcon Identity Threat Protectionがランサムウェア攻撃をどのように検知し阻止するかを、このビデオ（英語）でご覧ください。
- パワフルなCrowdStrike Falconプラットフォームで、組織、従業員、データをそれらの場所に関係なく、総合的に保護する方法をご紹介します。
- CrowdStrike Falcon Prevent™の無料トライアル版で、真の次世代型AVが、今日の非常に高度な脅威にどのように対抗できるかを体験してください。

原文：Buying IAM and Identity Security from the Same Vendor? Think Again.
https://www.crowdstrike.com/blog/why-you-shouldnt-buy-iam-and-identity-security-from-the-same-vendor/